PURPOSE *version: 2021-05*

*The objective of this form is to document the entity’s information system (IS) and communication relevant to the preparation of the financial statements. The engagement team can provide this template to the entity to complete. Alternatively, the engagement team may complete this document by making inquiries of relevant entity personnel and recording their responses below.*

1. Organisation and systems overview
   1. Main client contacts

*Indicate the main contact(s) for this engagement (Accounting and IT):*

| Individual's name | Title | Email | Telephone | Comments |
| --- | --- | --- | --- | --- |
| Henry Omal | Chief Accountant | accounts.office@lacorhospital.org | 0772 350123 |  |
| Joseph Laker | IT Manager | it.office@lacorhopital.org | 0772 012999 |  |
|  |  |  |  |  |

* 1. The IT function and IS Security function

*Briefly describe IT department organisation structure or attach the IT function organisation chart.*

|  |
| --- |
| The Department is currently comprised of 3 Staffs and 1 volunteer  IT Manager (1)  Senior IT Officer (1)  IT Officer (1) |

*Complete the following table, or provide an organisation chart, if the entity has one of the following:*

* *A dedicated IT department with structured IT processes supported by personnel that have software development and IT environment maintenance skills, or*
* *Use of internal service providers (e.g., group shared resources) to manage IT processes within, the entity’s IT environment (e.g., third-party hosting).*

| Name of key IT personnel | Position/role | Group / department within the IT Department | IT function |
| --- | --- | --- | --- |
| Joseph Laker | IT Manager |  | IT Infrastructure |
| Martin Akena Luluga | Senior IT Officer |  | Networks |
| Solomon Nono | IT Officer |  | Support |
|  |  |  |  |

* 1. Relevant IT suppliers or external service providers

*We consider relevant IT suppliers where the entity is outsourcing the hosting of its IT environment to a third party or using a shared service centre for central management of IT processes.*

| Service provider name | Service description - (also indicate whether they follow the entity’s processes OR their own processes and whether a SOC[[1]](#footnote-2) report is available) |
| --- | --- |
| PC World | No contract, No service outsourced but we refer to them in case we need external services especially in regards to Hardware |
|  |  |
|  |  |

* 1. Network infrastructure and security

*Briefly describe the entity’s IT network infrastructure or attach an infrastructure diagram.*

*The description and/or diagram includes elements such as:*

* *Use of cloud, web-facing application of a shared service centre*
* *Data centre location*
* *Remote access, including:*
  + *Whether key IT assets (e.g., applications, databases, folders or reports) are available through remote access and to whom they are available (e.g., internal users, clients, partners or everyone).*
  + *The name of the remote software in use*
* *Use of network management systems (e.g. Microsoft Active Directory, firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and/or other protection measures in place to protect the entity’s IT environment)*

|  |
| --- |
| Data centre is located within the hospital at two different locations (Primary Data Centre and Disaster Recovery)  Access to remote by remote users is controlled by the firewall (Barracuda Firewall), and authentication granted through the Active Directory (Microsoft). We use Barracuda Network Access Client (Barracuda VPN) to establish connection to remote users for resources physically located in Data centres located in the hospital. This is configured through a public IP address issued by our ISP. The key assets accessible by remote included Applications, and shared folders which are granted to some authorised partners, staffs at the foundation and internal users who may be out of the Hospital.  The firewall and web filter manages the network, and the Active directory authenticates the users but we also have a network monitoring systems (PRTG). |

* 1. Significant changes in IT environment

| Significant changes during the audited period | Brief description of change (or N/A) |
| --- | --- |
| Deployment of new financial/accounting applications  *(If question is answered Yes then complete 3.2.4)* | Clinic Master was introduced. The Introduction continues to move in a phased manner with Radiology getting ready for the next phase |
| Application end of life (i.e., planned end of application support, removal from use by the entity) | xCare system previously used in Radiology is getting replaced by Clinic Master |
| Major version(s) or upgrade(s) | Yes for Clinic Master, NA for Navision |
| Migration of data to a new system during the period |  |
| Significant IT projects undertaken by management that could affect the financial statements |  |
| Adoption of new technology that could affect the financial statements |  |
| Changes to service providers | NITA is being introduced alongside Roke ISP |
| *[Enter any additional significant changes here]* |  |

**Applications used by the entity**

* 1. List of applications / systems / data warehouses relevant for processing and recording of financial information

***For each business cycle, list in the table below the application(s) being used for processing and recording financial information.***

| Business cycle/ function | Application  (name of specific module if applicable)/ System / Data warehouse name and version | Version | Implemented/ upgraded during the year? | How is the application hosted? (entity’s server, a third party or shared service centre in a group) | Operating System | Database (including version) | Single Sign On | Type of application software | Configurable settings? |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Clinic Master | V 4.2.0 | Yes | Company's server | Microsoft Windows Server 2016 | SQL Server 2016 Database 13.0.4001.0 | No | Standard off-the-shelf |  |
|  | Microsoft Dynamic Nav | 2013 | No | Company's server | Microsoft Windows Server 2016 | SQL Database 13.0.4001.0 | No | Customised off-the-shelf |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |



1. Automation and use of data

*This section assists us to understand how data is entered into the system(s), the nature of the reports which are relevant to the audit and if financial data is automatically transferred between applications.*

* 1. Data Flow Diagram of financial reporting applications

*If available, please attach the organisation’s systems (applications) description, relevant interfaces, input, output and flow of data [replace example below]:*

|  |
| --- |
|  |

* 1. Main interfaces between applications that support the business cycles (*optional if 2.1 is completed)*
* *List all key interfaces between applications (i.e., those with a significant impact on the entity’s business processes and financial reporting).* *These include both interfaces within the entity and interfaces with external parties (e.g., Electronic Data Interchange (EDI), etc.).*
* *Provide details about each interface, such as the following:*

*1) fully automated, semi-automated or manual interface*

*2) nature of the data being transferred*

*3) if not fully automated, steps in place to perform the data transfer*

*4) controls to guarantee timely, accurate and complete data transfer (e.g. log review, exception reports, manual reconciliations, batch monitoring, etc.).*

| Interface applications | Details on the interface | Frequency (Batch, real-time, scheduled x times daily) |
| --- | --- | --- |
| *[Application 1] to [Application 2]* |  | Choose an item. |
|  |  | Choose an item. |
|  |  | Choose an item. |
|  |  |  |
|  |  | Choose an item. |
|  |  | Choose an item. |

* 1. Describe the use of complex technology components (for example blockchain, robotic processing automation (RPA), artificial intelligence, etc.), if any.

|  |
| --- |
| **NA** |

1. Description of IT processes
   1. Manage Access

3.1.1. Manage access process

*Briefly describe the manage access process and which organisation units are involved with respect to:*

* + *Operating system software*
  + *Network access*
  + *IT applications access and*
  + *Database access*

*If available mention existing internal procedures or attach a copy of the relevant procedure or reference it below.*

|  |
| --- |
| The hospital run Windows OS with access being granted through the Active Directory. All the Computers are joined to the hospital domain. There is a generic password for computers located at shared points (Reception, OPD Doctor’s Rooms, Wards). Computers assigned to specific individuals has password set as requested by the user. The application softwares installed on each computer depends on the department and the individual assigned to the computer.  Network access is automatic for computers on cabled connection with access to network resources controlled by the firewall and the web-filter. Wireless connection access is controlled by WPA security embedded on the Ubiquity Unifi controller hosted on one of the computes at the IP department.  Application access is based on user credential created from the server side. Installation and access is granted through request from the Head of Department and approval from the relevant authorities. Major applications with access rights are Microsoft Dynamics Navision and Clinic master. Each user has specific rights in line with the role they are assigned to.  Database access is restricted to frontend only for the user. The backend end is accessed by the IT department and the service providers on request. Access to backend is through management studio with the credential reserved to IT department. |

3.1.2. User accounts administration

* *Describe Administrators accounts for applications identified within the form that are accessible by single individuals.*
* *Describe if Administrator roles are defined*
* *Describe how user rights are set up (assigned individually, roles based on function etc.).*
* *Describe the method by which user accounts authenticate to the relevant applications / systems.*

|  |
| --- |
| Ever Users access different applications and have different rights/roles. Administrators accounts belongs to the IT department and management.  Administrator’s roles are defined. This is determined by the role played by the specified user of the application. This does not apply to the database and the developer’s environment of the applications used within the hospital.  User are assigned rights depending on the roles the play at the hospital. Different users have different rights. For instance, all users’ cashiers have transactional role in clinic master. Meaning their boundary stops at that.  Applications authenticate users through password-based authentication. Computers are authenticated using password via the AD. |

3.1.3 Authentication method to access IT resources

*Describe authentication methods and password policy as they apply to applications, operating systems and databases.*

| Application/ operating system/ databases | Password strength (document parameters or provide a screenshot of the settings) | Two factor authentication (i.e., token or SMS) (Y/N) |
| --- | --- | --- |
| Microsoft Windows OS | Depends on users (Users can change after a generic is set from the DC-AD) | *No* |
| Clinic Master | Depends on Users (User can modify after creation from the Administrator’s end) | No |
| Microsoft Dynamic Nav | Depends on Users (User can modify after creation from the Administrator’s end) | No |
| SQL Database | Strong – Alphanumeric (Reserved for IT department). | No |

* 1. Manage Change

*Describe how the entity manages program, database and operating system changes, if applicable. Such changes may be programmed in-house, performed by an IT consultant / external party, or processed by a software supplier.*

3.2.1 Describe how program, database and operating system change requests are submitted, evidenced, and approved by responsible personnel

|  |
| --- |
| Major changes in programs are determined by the top management with consultation from the IT advisory board from the Corti foundation and approval by the Hospital Board.  Changes in operating system for users is determined by the need and doesn’t require special approval provided it’s deemed necessary by the IT department. However, changes in server operating systems requires approval from the IT advisory board at the Corti foundation. |

3.2.2 Describe the use of separate IT environments for development, testing and production

|  |
| --- |
| The hospital has a test server and a IT laboratory dedicated for testing and training purpose. After a test is done and approval made, the system is deployed at the live/production environment. |

3.2.3 Regulatory or accounting changes impacting IT systems

*Describe changes that occurred during the period being audited relating to regulatory or accounting changes.*

|  |
| --- |
| NA |

3.2.4 Implementation of a new system relevant to financial reporting (see section 1.5 above)

*Describe changes that occurred during the period being audited relating to implementation of new systems relevant to financial reporting.*

|  |
| --- |
| NA |

* 1. IT Operations (Data processing)

*Describe how financial data is managed and processed by the IT Department through batch processing / job scheduling, including segregation of duties in the IT operations process*

|  |
| --- |
| Currently Lacor does not do data processing |

* 1. Other relevant IT processes

*Describe other IT processes, including data backup, continuity procedures and data centre physical security.*

3.4.1 Data backups and IT continuity

*Describe the process of creating a copy of the financial data to protect against accidental or malicious deletion, corruption, hardware failure, ransomware attacks, and other types of data loss.*

|  |
| --- |
| 1. A backup of the entire database is created locally using a scheduled maintenance plan, and copied to an offsite location 2. Using the SQL Always On availability service in SQL server, the the database is synchronized with the secondary server, which is located in a different location. 3. For continuity purposes, a failover can be activated to bring to production the secondary environment |

3.4.2 Physical security controls around data centres

*Describe the physical security controls applied to protect IT resources (e.g., hardware, software, network, and data) from natural disasters, burglary, theft, terrorism, and other events that could cause damage or loss to the entity’s financial data.*

|  |
| --- |
| The Server room is always locked. There are fire sensors in case fire explodes in the server room |

* 1. Security events and processes

3.5.1 Security vulnerability management process

*Describe your vulnerability management process using either internal or external parties (eg: asset inventory, vulnerability scan, vulnerability classification, patching and other remediation actions).*

|  |
| --- |
|  |

3.5.2 Cyber attacks / incidents

*Identify and list cyber attacks or incidents which may have compromised data, transactions or generated losses to the entity.*

*Describe briefly the root cause of the incident / problem and the entity’s response.*

| Incidents / problems | Applicable? | Description, root cause and impact |
| --- | --- | --- |
| Cyber attack | *No* |  |
| System disruption | *No* |  |
| Data loss | *No* |  |
| Delay in data processing / automated report preparation | *Yes* | Clnic Master faces delay in data processing. This is due to possible bug in data retrieval from the database. The service provider is working around to fix this. |
| Slow application change management | *No* |  |
| Problems during application data migration | *Yes* | Integration problem between CM and NAV |
| Known application functionality gaps – manual workaround needed | *No* |  |
| Other | Choose an item. |  |

1. System and Organisation Controls (SOC) reporting [↑](#footnote-ref-2)